

REMARKS

This Application has been carefully reviewed in light of the Office Action mailed March 25, 2005. Claims 1-23 were pending in the Application. In the Office Action, Claims 1-23 were rejected. Claims 1-23 remain pending in the Application. Applicants respectfully request reconsideration and favorable action in this case.

As an initial matter, Applicants have amended the paragraph beginning on page 1 of the specification to include cross-reference information to the serial numbers of the indicated applications. Applicants respectfully request favorable action regarding such amendment.

In the Office Action, the following actions were taken or matters were raised:

SECTION 102 REJECTIONS

Claims 1-23 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Publication No. 2002/0093527 issued to Sherlock et al. (hereinafter "*Sherlock*"). Applicants respectfully traverse this rejection.

Of the rejected claims, Claims 1, 9 and 16 are independent. Applicants respectfully submit that *Sherlock* does not disclose or even suggest each and every limitation of independent Claims 1, 9 and 16. For example, independent Claim 1 recites, at least in part, that "decoded data [related to an intrusion event and decoded to a predetermined format decipherable by humans] . . . comprises intrusion event data, data summary, and detailed data" and that such data is "present[ed] . . . to a user in an organized manner." The Examiner refers to paragraphs 0283, 0284 and Table H of *Sherlock* as disclosing the above-referenced limitation(s) (Office action, pages 2-3). Applicants respectfully disagree.

Sherlock appears to disclose a program, termed a "policy wizard," that makes an end user readily able to generate a first-pass security policy for a new site (*Sherlock*, paragraph 0098). For example, *Sherlock* appears to disclose that a user specifies a network security policy (e.g., via a set of dialog boxes) in terms of the network services provided by certain hosts to other hosts in the network (*Sherlock*, paragraphs 0098 and 0273). *Sherlock* also appears to disclose that the policy wizard generates a formal and more detailed description of

a network security policy using policy language (*Sherlock*, paragraph 0273). *Sherlock* further appears to disclose that the policy language specification may then be used to analyze network traffic using the policy monitor tool (*Sherlock*, paragraph 0273). *Sherlock* appears to disclose that the wizard translates the security policy into a set of policy language objects such as rules, credentials and dispositions (*Sherlock*, paragraph 0274). Tables F, G and H of *Sherlock* appear to disclose a set of predefined default rules for handling protocol events (*Sherlock*, paragraphs 0280-0282). In particular, “Table H . . . shows rules that cover protocol events not addressed by the wizard’s user interface” (*Sherlock*, paragraph 0282). Thus, the portion of *Sherlock* referred to by the Examiner appears to be a set of abstract rules that are applied to an event, and not decoded data relating to an actual intrusion event that comprises “intrusion event data, data summary, and detailed data” of such intrusion event as recited by Claim 1. Thus, Applicants submit that Table H of *Sherlock* does not disclose or even suggest the presentation of data of an intrusion event to a user that comprises “intrusion event data, data summary, and detailed data” of such intrusion event as recited by Claim 1. Therefore, for at least this reason, Applicants submit that *Sherlock* does not anticipate Claim 1.

The Examiner also refers to paragraph 0208 of *Sherlock* relating to an output option of the policy monitor of *Sherlock* as corresponding to “decoding the captured data from a predetermined format to a predetermined format decipherable by humans” recited by Claim 1 (Office Action, page 2). Applicants respectfully disagree. Paragraph 0208 of *Sherlock* recites:

Output options allow the end user to specify whether the trace output from the monitor should be displayed in a console window (Output to console) or sent to a file (Output to file).

(*Sherlock*, paragraph 0208)(emphasis added). Applicants respectfully submit that the recitation of a “trace output” by *Sherlock* as indicated above does not rise to the level required to support an anticipation rejection of Claim 1 under 35 U.S.C. § 102 where Claim 1 recites that the data presented to a user of an intrusion event comprises “intrusion event data, data summary, and detailed data.” To the contrary, *Sherlock* does not appear to explicitly identify what type of information is included in the “trace output,” nor has the Examiner explicitly identified any portion of *Sherlock* indicating the content of such “trace output.” Accordingly,

for at least this reason also, Applicants respectfully submit that *Sherlock* does not anticipate Claims 1.

Independent Claim 9 recites, at least in part, “capturing, from a network, data related to an intrusion event,” “decoding the captured data from a first predetermined format to a second predetermined format, the decoded data comprising network header data, data summary, and detailed data” and “presenting the decoded data according to a predetermined report format,” and independent Claim 16 recites, at least in part, “a network driver capturing data related to an intrusion event,” “a decode engine decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data comprising intrusion event data, data summary, and detailed data” and “a user interface presenting the decoded data to a user.” At least for the reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that *Sherlock* does not anticipate Claims 9 and 16.

Claims 2-8, 10-15 and 17-23 that depend respectively from independent Claims 1, 9 and 16 are also not anticipated by *Sherlock* at least because they incorporate the limitations of respective Claims 1, 9 and 16 and also add additional elements that further distinguish *Sherlock*. Therefore, Applicants respectfully request that the rejection of Claims 2-8, 10-15 and 17-23 be withdrawn.

CONCLUSION

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicants have overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By: 
James L. Baudino
Reg. No. 43,486

Date: June 23, 2005

Correspondence to:
L.Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400
Tel. 970-898-3884